

WHAT IS CLAIMED IS:

1. A right-information distribution method comprising the steps of:

generating right information and verification information for authenticating the validity of a portable electronic device when the right information is stored in said portable electronic device;

generating a right code, which is provided offline, by encrypting the right information and the verification information;

inputting the offline-provided right code to said portable electronic device;

decrypting the input right code and using the verification information to authenticate the right information based on the decrypted right code; and

storing the authenticated right information in said portable electronic device.

2. A right-information distribution method according to Claim 1, wherein the right information includes information which permits admission to a predetermined place.

3. A right-information distribution method according to Claim 1, wherein said portable electronic device is an

integrated circuit card.

4. A right-information distribution method according to Claim 1, wherein the step of inputting the offline-provided right code to said portable electronic device is performed by an information management apparatus.

5. A right-information distribution method according to Claim 4, wherein the storing of the right information is performed when said portable electronic device and said information management apparatus are combined with each other.

6. A right-information distribution method according to Claim 1, further comprising the steps of:

inputting a first right code added to the right information, and an identification number for returning the right information to a source of the right information; and after confirming the input first right code and the input identification number, confirming an offline-providable second right code for returning the right information to said source of the right information, and invalidating said first right code.

7. A right-information distribution method for

transferring right information from a first portable electronic device to a second portable electronic device, said right-information distribution method comprising the steps of:

generating the right information and verification information for authenticating the validity of said first portable electronic device when the right information is stored in said first portable electronic device;

generating a first right code, which is provided offline, by encrypting the right information and the verification information;

inputting the offline-provided first right code and the identification number of said second portable electronic device to said first portable electronic device;

after confirming the input first right code and the input identification number, invalidating the first right code and generating a second right code, which is provided offline;

inputting the second right code to said second portable electronic device;

decoding the input second right code and authenticating the decoded second right code; and

storing, in said second portable electronic device, the right information which is included in the authenticated second right code.

8. An information distribution system comprising:  
a portable electronic device for a user; and  
an information management apparatus for storing both  
information on a predetermined right and information  
corresponding to said portable electronic device, the second  
information indicating to whom a right belongs;

wherein:

said information distribution system manages the  
location of said right by updating the right information  
stored by said information management apparatus and the  
information indicating to whom said right belongs;

said information management apparatus comprises:

information holding means for holding the right  
information;

access means for recording the transfer of said  
right to said user by accessing said information holding  
means and for updating the right information held by said  
information holding means;

encryption means for generating encrypted  
information by using a code unique to said portable  
electronic device to encrypt the information indicating to  
whom said right belongs to be in an offline provable form;  
and

information providing means for providing said user

with the encrypted information so that the encrypted information passes through an offline channel at least once; and

    said portable electronic device comprises:

        input means for accepting the input of the encrypted information;

        decryption means for decrypting the encrypted information using said unique code and outputting the information indicating to whom said right belongs;

        recording means for recording the output information indicating to whom said right belongs; and

        information output means for using a predetermined access means to output the recorded information indicating to whom said right belongs.

9. An information distribution system according to Claim 8, wherein said information indicating to whom said right belongs is information for permitting admission to a predetermined place.

10. An information distribution system according to Claim 8, wherein said information management apparatus executes billing in response to the provision of the encrypted information by said information providing means.

11. An information distribution system according to  
Claim 8, wherein:

    said portable electronic device comprises:

        information generating means for generating  
        information for requesting the transfer of said right based  
        on the information recorded in said recording means;

        encryption means for generating encrypted transfer  
        information by using a code unique to encrypt the  
        information for requesting the transfer of said right so  
        that the encrypted transfer information is provided offline;

        control means for controlling the accessing of the  
        information recorded in said recording means in response to  
        the encryption by said encryption means; and

        output means for outputting the encrypted transfer  
        information so that the encrypted transfer information  
        passes through an offline channel at least once; and

    said information management apparatus further comprises  
    a decryption means for decrypting the encrypted transfer  
    information, and updates right information which corresponds  
    to the output of said decryption means by using said access  
    means to access said information holding means in response  
    to the output of said decryption means.

12. An information distribution system according to  
Claim 11, wherein said information management apparatus

executes billing in response to the provision of the encrypted information by the information providing means, and changes the billing in response to the encrypted transfer information.

13. An information distribution system according to Claim 11, wherein:

    said portable electronic device comprises:

        encryption means for generating second encrypted information based on the information recorded in said recording means by using a code unique to another portable electronic device so that the second encrypted information is provided offline;

        control means for controlling the accessing of the information recorded in said recording means in response to the encryption by said encryption means; and

        output means for outputting the second encrypted information so that the second encrypted information is provided to the other portable electronic device after passing through an offline channel at least once; and

    the other portable electronic device performs the processing of the second encrypted information, which is identical to the processing of the encrypted information by said portable electronic device.

14. An information management method for, by updating right information held by an information management apparatus and by recording in a portable electronic device information indicating to whom said right belongs, managing said right so as to be exercised when said portable electronic device is with a user, wherein said information management method controls said information management apparatus to perform the steps of:

generating encrypted information to be in an offline provable form by using a code unique to said portable electronic device to encrypt the information indicating to whom said right belongs; and

providing said user with the encrypted information so that the encrypted information passes through an offline channel at least once.

15. An information management method according to Claim 14, wherein the billing is performed in response to the provision of the encrypted information.

16. An information management method according to Claim 14, wherein said information management method controls said portable electronic device to perform the steps of:

generating encrypted transfer information by using a

unique code to encrypt information for requesting the transfer of said right so that the encrypted transfer information is provided offline; and

preventing the information indicating to whom said right belongs from being output, and transmitting the encrypted transfer information to said information management apparatus so that the encrypted transfer information passes through the offline channel at least once.

17. An information management method according to Claim 16, wherein said information management method controls said image management apparatus to perform the steps of:

executing a billing process in response to the provision of the encrypted information; and

changing said billing process in response to the encrypted transfer information.

18. An information management method according to Claim 14, wherein said information management method controls said portable electronic device to perform the steps of:

generating second encrypted information based on the information indicating to whom said right belongs by using a code unique to another portable electronic device so that

the second encrypted information is provided offline; and providing the second encrypted information to the other portable electronic device so that the second encrypted information passes through the offline channel at least once; and

outputting the second encrypted information and preventing the information indicating to whom said right belongs from being output.

19. An information management method according to Claim 18, wherein said portable electronic device is an INTEGRATED CIRCUIT card.

20. An information management method according to Claim 18, wherein the information indicating to whom said right belongs is information for allowing said user to enter an event place.